Arizona State Treasurer's Office
Local Government Investment Pool
Internet Participant Access System
(LGIP-IPAS)
Liability Limitations

This document addresses several issues that affect liabilities arising from the offer and acceptance of remote, electronic access to the IPAS system. This document recognizes the risks already described and agreed to in the Risk Acknowledgement, but attempts to more clearly clarify the duties associated with system use.

Authorization

IPAS authorization is separate and distinct from call-in authorization. As such, IPAS users cannot call the Arizona State Treasurer's Office and place verbal transaction requests unless they are also authorized for call-in.

Similarly, IPAS user accounts and passwords are unique and issued to each user individually. These accounts and passwords should not be shared with any other staff member. Passwords were created in a manner to make it more difficult for others to guess. Participant must be sure not to write it down in a place that others would be likely to find it. The Arizona State Treasurer's Office has put procedures in place to ensure that internal staff does not have access to Participant user passwords.

Initial passwords will be assigned by the Arizona State Treasurer's Office Security Staff, with the password being transferred to the user out-of-band. Any password change requests need to be addressed to ASTO Security Staff at ipas@aztreasury.gov. Password changes will not be given via phone, and the email address and contact numbers used by ASTO Security Staff to contact the Participant will only be the ones listed on the authorization form.

Upon the event that an authorized user terminates their employment, Participant is responsible to notify Arizona State Treasurer's Office personnel of such a change in a timely fashion. Until such notice is received, all user rights will be retained at their previous levels.

Security

The Arizona State Treasurer's Office has developed a System Security Program and System Architecture designed for reliability and to protect Participant’s data from unauthorized access. The ASTO maintains updated inventories of all hardware and software, as well as diagrams showing the design and connectivity of the network components. For audit purposes, these items are available for Participant review at the Arizona State Treasurer's Office during normal business hours, but cannot be copied or removed from the premises.

Additionally, The Arizona State Treasurer's Office has ensured that all critical data processing equipment is maintained in a physically secure environment to reduce the likelihood of

environmental damage or inappropriate access to Participant information systems by employees, contractors, service providers, other Participants and others. The physical security systems include access control devices, monitoring systems, environmental control systems and protection systems.

It is up to the individual Participant to ensure the general security over any personal computer utilized to access the IPAS system. General security responsibilities include ensuring proper authentication controls, virus protection, mal-ware detection, patch management and physical access controls. Participant will need to contact their IT support staff if they have any questions concerning the current state of their system security.

In order to ensure the greatest level of security possible for Participants utilizing the IPAS system, it is imperative that Participants notify the Arizona State Treasurer's Office at the soonest possible time regarding any concern they might have about their online access, unauthorized transactions, loss or theft of access methods, or any other information that Participant is aware of that might negatively affect the security of the IPAS system.

Encryption

Encryption is the process of scrambling private information to prevent unauthorized access. To show that your transmission is encrypted, some browsers display a small icon on your screen that looks like a “lock” or a “key” whenever you conduct secure transactions online.

The IPAS system uses encryption to ensure transaction data privacy and security in transit. Additionally, IPAS uses a secure server identification certificate to allow authentication that the Participant has connected to the IPAS server supported by the Arizona State Treasurer's Office.

It is incumbent upon the Participant to notify the Arizona State Treasurer's Office if they have any issues or difficulties connecting to the IPAS system securely. Any transactions sent without the proper encryption creates a vulnerability to Participant data.

Social Engineering

The Arizona State Treasurer's Office would like to ensure that Participants do not fall victim to social engineering attacks. Social engineering is an attempt by unauthorized individuals to gain access to a system by inducing employees into providing their account information to them. They do this through various methods, including phone calls purporting to be from a security staffer, phishing and pharming attacks via email, and through the use of copycat web sites that deliberately attempt to mislead a user.

To prevent these attacks from being successful, the Arizona State Treasurer's Office will never contact you via email or phone to request any login or user information regarding IPAS, nor will we include any link in an email requesting you to log into our system or make any affirmative action.

It is the responsibility of the Participant to train and inform their staff so that any such requests will be recognizable as social engineering attempts. Any such attempt received should be reported immediately to the proper local authorities and to the Arizona State Treasurer's Office. Participant should capture and retain as much information as possible regarding the attack as this will aid in the identification of persons who commit or attempt such attacks.

Transactions

The IPAS system is an additional mechanism to enter transaction requests for Participant's LGIP accounts. As such, it is intended to be in addition to, and not a replacement of, existing access methods. Because of this, the Arizona State Treasurer's Office does not guarantee or certify that access to the system will always be available. Any unavailability of the system does not create any additional liability on the part of the Arizona State Treasurer's Office over that which already exists through the existing access methods.

By utilizing the IPAS system, Participant is aware that IPAS operates on a real-time basis. Any transactions entered and approved are automatically effective on the Participant's account. Any transactions created through the other existing access methods (call-in, via fax, email, etc) are handled on a batch process basis, and will not immediately be reflected on your account on IPAS.